

Listing and Amendments to the Claims

This listing of claims will replace the claims that were published in the PCT Application:

1. (currently amended) Method for decrypting data within a device, the data comprising a an encrypted first data set and a an encrypted second data set, ~~the first and second data set being encrypted~~, wherein said first data set ( $AV_E$ ) and a respective device independent electronic decryption key ( $K_3$ ) are stored on a removable ~~read-only~~ prerecorded storage medium ( $D$ ), and the second data set ( $SD_E$ ) is not stored on ~~said the~~ removable ~~read-only~~ prerecorded storage medium ( $D$ ) but is related to the first data set ( $AV_E$ ), ~~characterized in the method comprising the steps of~~
  - retrieving the first data set ( $AV_E$ ) ~~from the removable read-only~~ and the device independent decryption key from the removable storage medium ( $D$ );
  - ~~retrieving the decryption key ( $K_3$ ) from the removable read-only storage medium ( $D$ )~~;
  - retrieving the second data set ( $SD_E$ ) from a second data source ( $IN$ );
  - decrypting ~~said the~~ first data set ( $AV_E$ ) using said decryption key ( $K_3$ ); and
  - decrypting ~~said the~~ second data set ( $SD_E$ ) using said decryption key ( $K_3$ ).
2. (currently amended) Method according to claim 1, ~~wherein the first data set ( $AV$ ) comprises at least audio-visual data, and the second data set ( $SD$ ) is a supplementary data set~~, further comprising the step of determining from a plurality of data sets on the second data source a second data set that refers to the removable storage medium, wherein the data sets refer to different removable prerecorded storage media.
3. (currently amended) Method according to claim 1 ~~or 2~~, further comprising the step of detecting whether the removable storage medium and the second data set are authorized by the same authority, wherein the second data set ( $SD$ ) ~~comprises one or more of subtitle, audio, video or graphics data, playlists, movie objects,~~

- ~~executables, bonus tracks, games or screen savers.~~ is regarded as authorized if it can be decrypted by said decryption key.
4. (currently amended) Method according to ~~any of the previous claims~~ claim 1, wherein the electronic decryption key (~~K3~~) is only accessible while a removable ~~read-only prerecorded~~ storage medium (~~D~~) that contains said electronic decryption key (~~K3~~) is readable.
5. (currently amended) Method according to ~~any of the previous claims~~ claim 1, wherein two or more electronic decryption keys (~~K1, K2~~) are stored on the removable ~~read-only prerecorded~~ storage medium, wherein at least one of said keys can be used for decryption of the first data set (~~AV<sub>E</sub>~~) and another of said keys can be used for decryption of the second data set (~~SD<sub>E</sub>~~).
6. (currently amended) Apparatus for decrypting ~~a data set~~ data within a device, the data set comprising a an encrypted first data set and a an encrypted second data set, ~~the first and second data set being encrypted~~, wherein said first data set (~~AV<sub>E</sub>~~) and a respective device independent electronic decryption key (~~K3~~) are stored on a removable ~~read-only prerecorded~~ storage medium (~~D~~), and the second data set (~~SD<sub>E</sub>~~) is not stored on said ~~thermovable read-only prerecorded~~ storage medium (~~D~~) but is related to the first data set (~~AV<sub>E</sub>~~), ~~characterized in that~~ the apparatus ~~comprises comprising~~
- means for retrieving the first data set (~~AV<sub>E</sub>~~) ~~from the removable read-only and~~ the device independent decryption key from the removable storage medium (~~D~~);
  - ~~—means for retrieving the decryption key (K3) from the removable read-only storage medium (~~D~~);~~
  - means for retrieving the second data set (~~SD<sub>E</sub>~~) from a second data source (~~IN~~);
  - means for decrypting said first data set (~~AV<sub>E</sub>~~) using said decryption key (~~K3~~);
  - and
  - means for decrypting said second data set (~~SD<sub>E</sub>~~) using said decryption key (~~K3~~).
7. (currently amended) Apparatus according to claim 6, further comprising ~~local storage means (HD) for storing said first or second data set, or parts of said first or second data set, before decryption~~ for determining from a plurality of data sets on the

second data source a second data set that refers to the removable storage medium,  
wherein the data sets refer to different removable prerecorded storage media.

8. (currently amended) Method or apparatus according to ~~any of the previous claims~~  
claim 1, wherein the electronic decryption key ( ~~$K_3$~~ ) is the only suitable key for  
decrypting the first data set ( $AV_E$ ), but is one of several suitable keys for  
decrypting the second data set ( $SD_E$ ).

Claim 9 is cancelled.

10. (currently amended) Method or apparatus according to ~~any of the previous  
claims~~ claim 1, wherein the first and second data sets are encrypted using RSA  
(Rivest-Shamir-Adelman) coding.

11. (new) Apparatus according to claim 6, further comprising means for detecting  
whether the removable storage medium and the second data set are authorized by the  
same authority, wherein the second data set is regarded as authorized if it can be  
decrypted by said decryption key.